

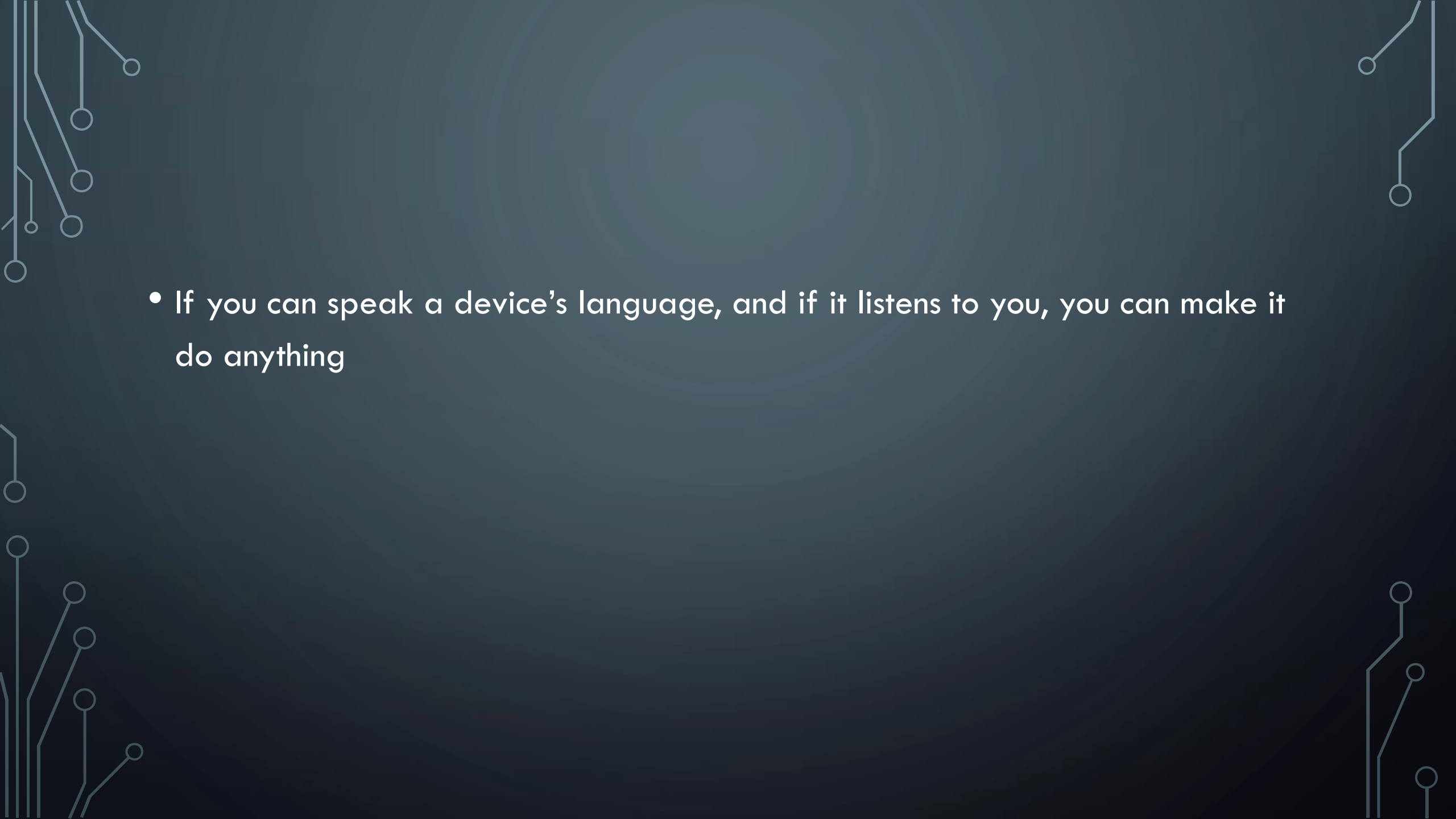


# HACKING A CLOUDPET

THE DANGERS OF INSECURE IOT

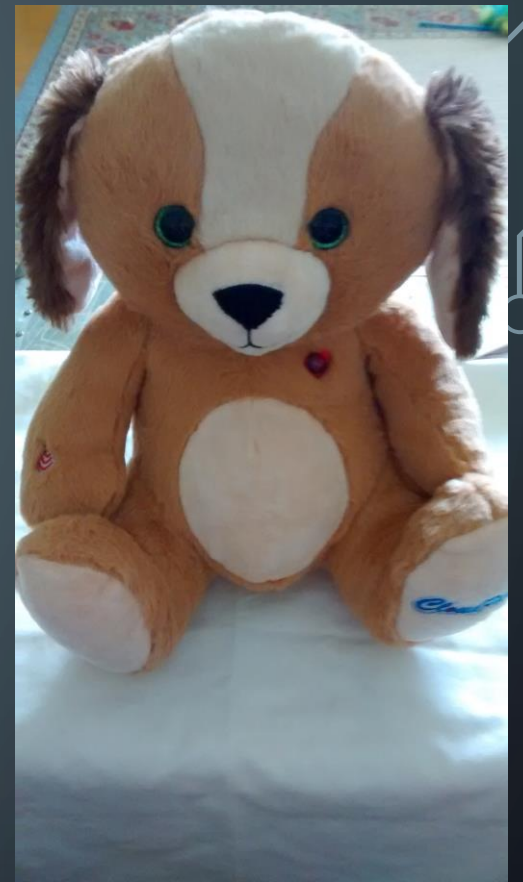
# ABOUT ME - KOREY YOUNG

- Bloomsburg University – Computer Science.
- But I have always had an interest in cyber security and hacking / red team activities
  - Finding ways to make computers do things that they were not meant to do;
  - So that we can get it fixed before the bad guys discover it and try to use it.
- Dakota State University - Masters in Information Assurance
- My day job is cyber security for an electric utility in the area, doing penetration testing on our applications, and scanning/monitoring our network for badness.
- In my free time after work and on weekends, I do cyber security and exploit research.

- 
- The background is a dark blue gradient. In the corners, there are white line-art illustrations of circuit boards or neural networks, with lines connecting to small circles.
- If you can speak a device's language, and if it listens to you, you can make it do anything

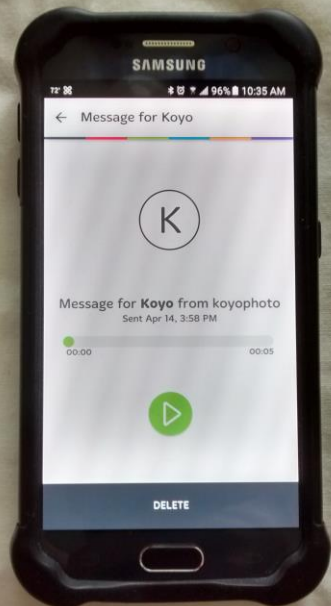
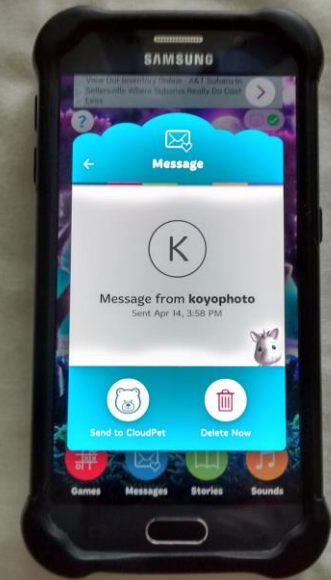
# HACKING A CLOUDPET

- Cloudpet: a stuffed animal that can play recordings sent from a phone app, and can record audio and send it back to your phone app.
- This little guy had little to no security built in - unencrypted communications, inability to patch, etc.
- Project for Master's class, using tutorial from security research org
- Surreptitiously record audio (no normal recording light) via rouge device
- Trigger audio play back on the cloud pet via rouge device.
- Send the recording to rouge device.



# NORMAL CLOUDPET INTERACTION

- Normally interact with the cloudpet using the cloudpet phone app
- Record audio messages on the phone app and send to the cloudpet to play
- Record audio messages on the cloudpet and send to the phone app to play





# NORMAL CLOUDPET INTERACTIONS

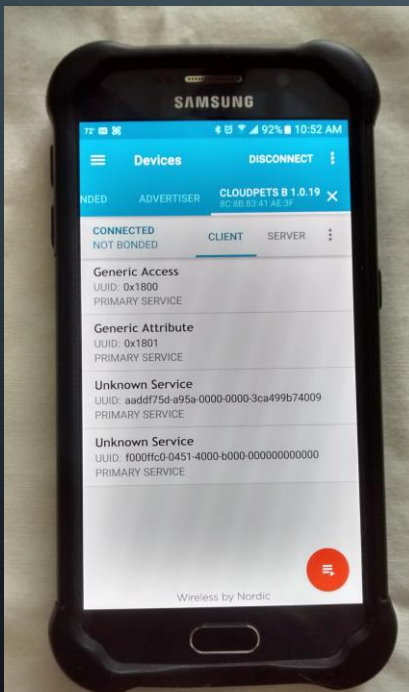
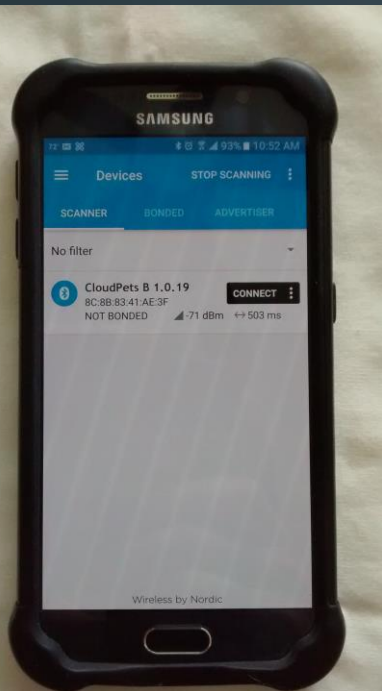
- Click on the blue button on the arm to play audio sent from the phone app
- Click on the red button on the other arm to record audio and send it to the phone app



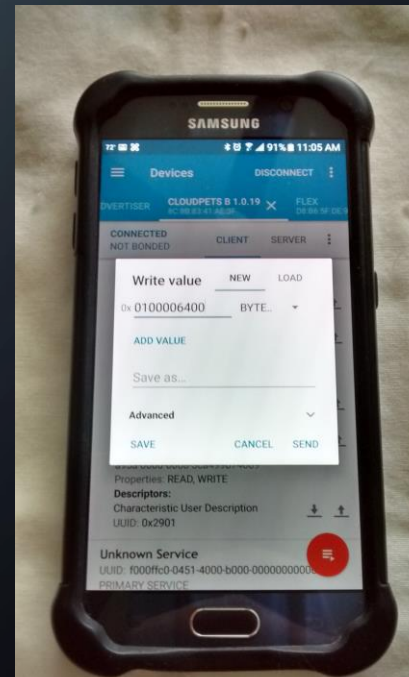
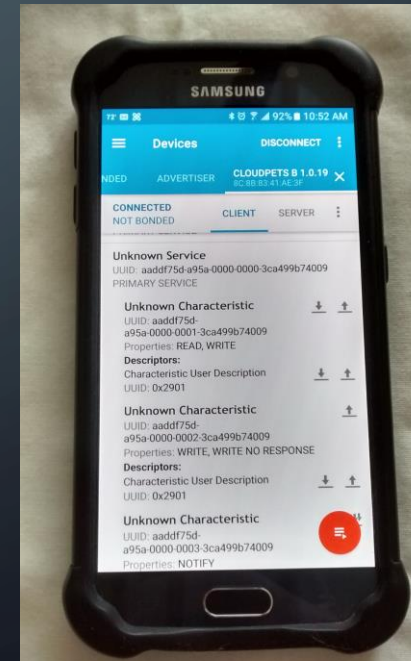
# SUBVERSIVE INTERACTION

- You can pick up the cloudpet's Bluetooth signal using a Bluetooth RF phone app
- The cloudpet will present data and available interactions to the RF phone app

Characteristic UUID	User Description	Properties
AADD75D-A95A-0000-0001-3CA499B74009	Command	Read, Write
AADD75D-A95A-0000-0002-3CA499B74009	Audio Write	Write
AADD75D-A95A-0000-0003-3CA499B74009	Return Audio	Notify
AADD75D-A95A-0000-0004-3CA499B74009	State	Read, Notify
AADD75D-A95A-0000-0005-3CA499B74009	Data Request	Read, Notify
AADD75D-A95A-0000-0006-3CA499B74009	Config	Read, Write
AADD75D-A95A-0000-0007-3CA499B74009	LED	Read, Write
AADD75D-A95A-0000-0008-3CA499B74009	Volume	Read, Write



- Send data with the RF phone app to the cloudpet, and the cloudpet will accept the interaction instructions



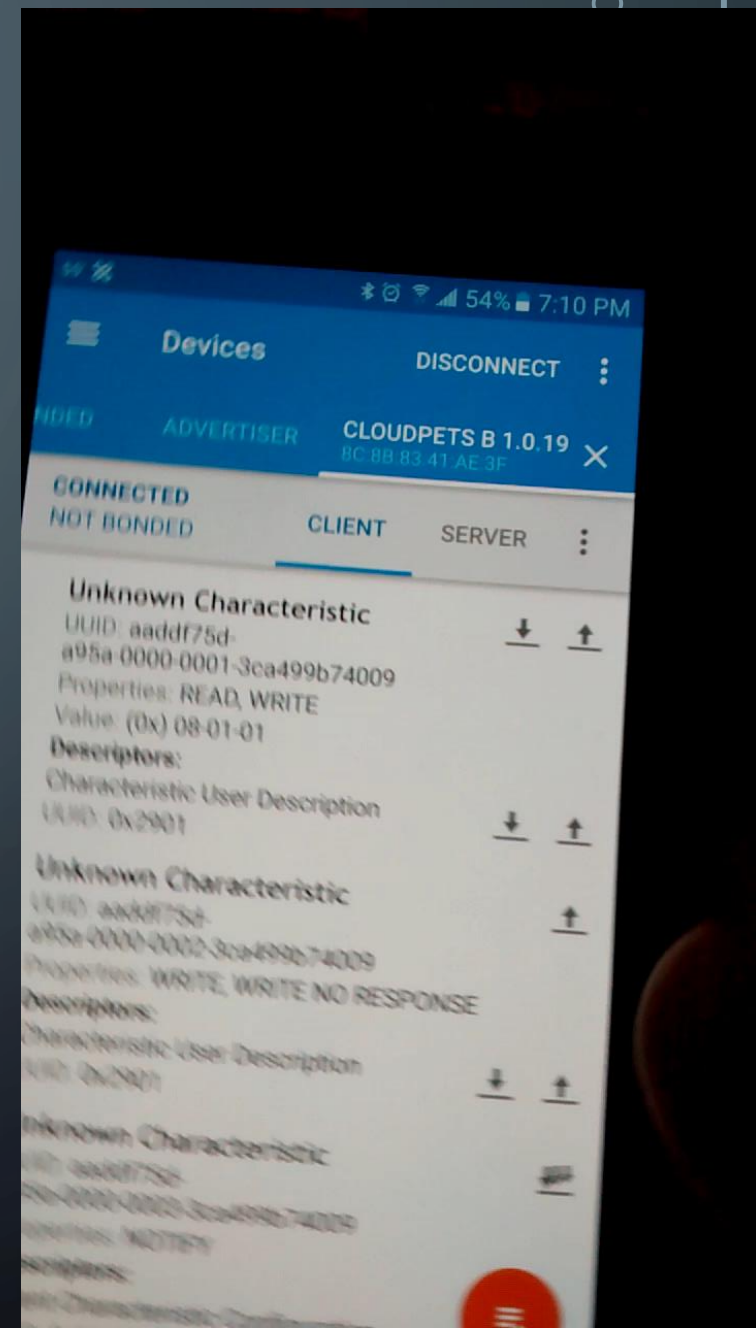
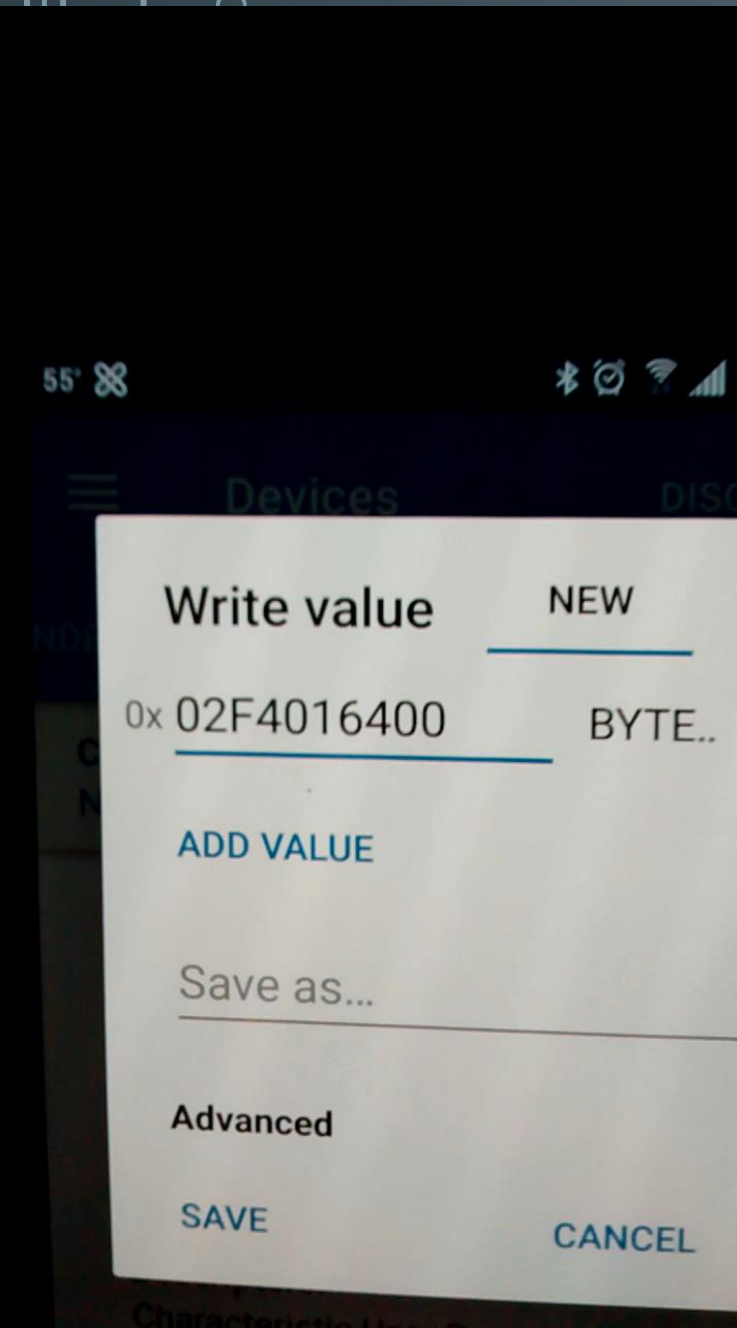
# SUBVERSIVE INTERACTION

- Play audio without user interaction
  - Creep someone out
- Record audio without user interaction
  - Creep someone out / Eavesdrop
- Record audio without normal recording light
  - Eavesdrop
- Make light blink





# DEMO VIDEOS



# DEMO

- Commands – nRF app: service 74009
  - audio recording – characteristic 1
    - 080102 - play back recording from phone app
    - 080100 - stop play back
    - 080200 - record on CloudPet with light off
    - 080101 - play back recording from CloudPet
  - led light – characteristic 7
    - 02f4016400 - blink
    - 0000006400 - off
    - 0100006400 - on

# IOT INSECURITY

- IOT in general has many of these security issues
  - unsecure communications
  - no way to patch vulnerabilities
  - easy to guess default username and password, or no username or password
  - devices sitting unprotected on the internet
  - and more
- The world got a lesson on the dangers of IOT insecurity when the Mirai botnet used insecure IOT devices to launch huge DDOS attacks
  - Accidentally took out DNS provider DYN, which in turn took out major internet sites such as Twitter, the Guardian, Netflix, Reddit, CNN, and more.
- If IOT security does not get bolstered soon, there will be many more IOT attacks in the future.

# CONCLUSION / TAKEAWAYS

- Internet and app connected devices can be dangerous if not properly secured
- The device itself can be hijacked or harmed
- The device can be used to harm other devices
  - If the device is connected to your broader network, an attacker could pivot to other devices on the network and compromise the other devices
  - The device can be used to send traffic and overwhelm other devices even outside your network (normal traffic allowed outside your firewall)
- Don't be afraid to research: if you have an interest, obtain a test device or set up a lab environment and explore how it works.



# QUESTIONS?

